

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

AMY COULSON,

Plaintiff,

v.

CHANGE HEALTHCARE INC., OPTUM,
INC., and UNITEDHEALTH GROUP
INC.,

Defendants.

Case No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Amy Coulson, individually and on behalf of all others similarly situated, alleges the following based on her personal experience and the investigation of counsel:

INTRODUCTION

1. Plaintiff brings this proposed class action lawsuit against Defendants Change Healthcare Inc. (“Change Healthcare”), Optum, Inc. (“Optum”), and UnitedHealth Group Inc. (“UnitedHealth,” collectively with Change and Optum, “Defendants”), for their negligent failure to protect the sensitive and confidential personally identifiable information (“PII”) and personal health information (“PHI”) of millions of patients across the United States. Their negligence resulted in the theft for ransom, on February 21, 2024, of the PII and PHI of millions of United States citizens, and left millions of patients unable to obtain their necessary medications for weeks or months. Their negligence also resulted in thousands of hospitals, clinics, doctors, pharmacies, and other healthcare providers going unpaid for weeks or months.

2. Defendants operate an enormous clearinghouse that processes between one-

third and one-half of all healthcare insurance claims in the United States. Defendants process approximately 15 billion healthcare insurance claims per year with a combined value of more than \$1.5 trillion per year—roughly 5% of the annual gross domestic product of the United States. And their data systems held the PII and PHI of approximately 100 million United States citizens—roughly 1/3 of all Americans.

3. Defendants were well aware that the enormous trove of sensitive personal data they possessed would be an irresistible target for cyberthieves. They had been warned by the United States government that there were at least 70 cyberattacks since December 2023, mostly against healthcare organizations.

4. But Defendants, despite knowing the risks, failed to take even the most basic precautions to protect the sensitive PII and PHI held in their data systems. It has long been understood that a simple username and password provide almost no security because they can easily be stolen or hacked. Accordingly, nearly every online transaction involving sensitive information now requires multifactor authentication.

5. Yet on February 21, 2024, a dark web entity known as BlackCat or AlphV (“BlackCat”) was able to steal the PHI and PII of 1/3 of the population of the United States because they obtained a compromised username and password and *nothing more was required* to access Defendants’ data systems. Most people in the U.S. cannot view their own bank statements without passing through more stringent security than Defendants required. Defendants failed to institute even the most basic security measures, essentially leaving the door open for cyberthieves. In fact, the thieves had been

wandering around undetected in Defendants' data systems for weeks before they struck.¹

6. Once Defendants became aware of the cyberattack, they immediately shut down their entire network to prevent further damage. This meant that roughly 40 million healthcare transactions went unprocessed every day the system was shut down. Indeed, some services are still not functioning,² and others took weeks to return to service.³ This is at least in part due to Defendants' negligent failure to institute a Business Continuity Plan, and a Disaster Recovery Plan. These widely used protocols are designed to minimize the impact of cyberattacks by maintaining redundant, secure backup systems offline that enable a rapid rebuild of the hacked data systems, among other steps.

7. As a direct result of Defendants' negligence, the PII and PHI of approximately 100 million U.S. citizens are now in the hands of cybercriminals, leaving those individuals vulnerable to identity theft and other injuries for the foreseeable future. And millions of patients throughout the United States, including Plaintiff, were and are unable to access the healthcare and medications they need. In addition, thousands of healthcare providers have suffered financial harm because they have not received the insurance payments they rely on to keep their businesses solvent. Plaintiff, individually and on behalf of all others similarly situated, alleges claims for negligence, negligence

¹ See, Testimony of Andrew Witty Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations “Examining the Change Healthcare Cyberattack,” May 1, 2024, at 3, available for download at <https://www.congress.gov/118/meeting/house/117242/witnesses/HHRG-118-IF02-Wstate-WittyS-20240501-U5.pdf> (“Witty Testimony”).

² See <https://solution-status.optum.com/>.

³ See, <https://www.unitedhealthgroup.com/ns/changehealthcare.html>.

per se, and unjust enrichment against Defendants, and seeks all available monetary and equitable relief.

PARTIES

8. Amy Coulson is a resident and citizen of Arlington, Tennessee in Shelby County. Ms. Coulson was unable to purchase medications she relies on to treat serious medical conditions as a result of Defendants' negligence.

9. Defendant UnitedHealth Group Incorporated ("UnitedHealth") is a Delaware Corporation with its principal place of business in Minnetonka, Minnesota. United is a vertically integrated enterprise with several wholly owned subsidiaries, including Change Healthcare and Optum.

10. Defendant Change Healthcare Inc. is a Delaware corporation with its headquarters in Nashville, Tennessee. It was acquired by UnitedHealth in 2022 and merged with OptumInSight that same year.

11. Defendant Optum, Inc. ("Optum") is a Delaware corporation with its headquarters in Eden Prairie, Minnesota. Optum provides healthcare technology, analytics and services to United Healthcare, the largest commercial health insurer in the United States (and another subsidiary of UnitedHealth), among others.

JURISDICTION AND VENUE

12. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated claims of the individual class members exceed the sum or value of \$5,000,000, exclusive of interests and costs, and this is a class action in which one or

more members of the proposed class, including Plaintiff, are citizens of a state different from Defendants. The Court has supplemental jurisdiction over the alleged state law claims under 28 U.S.C. § 1337 because they form part of the same case or controversy.

13. Venue is proper in this District under 28 U.S.C. § 1331 because Defendants Change Healthcare has its headquarters within this district, Plaintiff resides in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Background

14. Change Healthcare is a healthcare technology company that offers health care providers, pharmacies, and insurance companies claims and reimbursement management, billing solutions, and prescription processing. It is the largest processor of healthcare insurance claims in the country.

15. Change Healthcare as it exists today is the product of a rapid succession of acquisitions over a relatively short time period. This exponential growth was enabled by the passage of the Health Insurance Portability and Accountability Act (“HIPAA”) in 1996.

16. HIPAA was enacted, in part, “[t]o improve the efficiency and effectiveness of the health care system.”⁴ In addition to establishing privacy and security standards for PHI and PII (which Defendants failed to comply with), HIPAA included administrative

⁴ <https://www.hhs.gov/hipaa/for-professionals/index.html>.

simplification provisions intended to encourage the electronic transmission and processing of health care claims. Prior to its passage, health care claims were transmitted via paper and fax; transmission was slow and unreliable.⁵

17. After HIPAA became law, myriad small companies emerged that facilitated the electronic transmission and processing of health care claims, acting as intermediaries between the healthcare providers and the large insurance companies and health plans that lacked the expertise and agility to capitalize on the new law. These intermediary companies are called “clearinghouses.”

18. Eventually, a health tech “roll up” called Emdeon began acquiring many of these clearinghouses and related companies, purchasing or merging with 18 different companies, including Change Healthcare, whose name it adopted in 2014. As a healthcare non-profit recently described it, Emdeon/Change Healthcare is:

an agglomeration of the acquired companies’ IT systems, with hundreds of thousands of user interfaces and vast interconnected databases[,] . . . an immense kluge of IT infrastructure, a pulsing circulatory system through which flows billions of dollars a day in medical payments. It may be the most lucrative cyberterrorism target in the US economy.⁶

19. In 2021, OptumInsight, a subsidiary of UnitedHealth, purchased Change Healthcare (f/k/a Emdeon) for \$13 billion. Optum is itself a conglomeration, having acquired or merged with 18 other companies (in addition to Change Healthcare) since its

⁵ Jeff C. Goldsmith, *Will The Change Healthcare Incident Change Health Care?*, March 15, 2024, available for download at <https://www.healthaffairs.org/content/forefront/change-healthcare-incident-change-health-care>.

⁶ *Id.*

creation in 2011. The deal was opposed by the DOJ, but a federal district court approved the acquisition over the DOJ's objections. In its complaint, the DOJ described Change Healthcare as:

the nation's largest electronic data interchange (EDI) clearinghouse, which transmits data between healthcare providers and insurers, allowing them to exchange insurance claims, remittances, and other healthcare-related transactions . . . It has access to a vast trove of competitively sensitive claims data that flows through its EDI clearinghouse—over a decade's worth of historic data as well as billions of new claims each year.⁷

20. Moreover, according to the DOJ,

50 percent of all medical claims in the United States pass through Change's EDI clearinghouse. Change's self-described 'pervasive network connectivity,' including approximately '900,000 physicians, 118,000 dentists, 33,000 pharmacies, 5,500 hospitals and 600 laboratories,' means that even when United's health insurer rivals choose not to be a Change customer, health insurers have no choice but to have their claims data pass through Change's EDI clearinghouse. Not only does Change process vast amounts of competitively sensitive claims data, but it also has secured 'unfettered' rights to use over 60 percent of this data for its own business purposes including, for example, using claims data for healthcare analytics. Additionally, through its claims editing product, Change has access to the proprietary plan and payment rules for all of United's most significant health insurance competitors.⁸

21. According to the Change Healthcare website, its "extensive network, innovative technology, and expertise inspire a stronger, better coordinated, increasingly

⁷ *United States v. UnitedHealth Group Incorporated*, Case No. 1:22-cv-00481 (D.D.C.), Complaint, at 5.

⁸ *Id.*, at 4.

collaborative, and more efficient healthcare system.” It bills itself as a “trusted partner for organizations committed to improving the healthcare system through technology.”⁹

22. Change Healthcare also represents to providers that its “advanced technology and services helps [them] enhance patient engagement and access, improve outcomes, drive revenue performance, and improve operational efficiency.” Change Healthcare represents to payers that its “advanced technology solutions and services help payers achieve their priorities across the member journey.” Change Healthcare promises its partners that its “advanced technology solutions empower our partners to achieve their strategic business objectives and meet their customers’ needs.” And it assures patients that its “solutions streamline the engagement, care, and payment experience to improve the patient journey.”¹⁰

Defendants Failed to Take Adequate, Industry-Standard, and Statutorily-Required Precautions to Protect PHI and PII of Plaintiff and the Class.

23. For companies that handle large amounts of PHI and PII, including Defendants, the risk of cyberattacks is omnipresent. Typically, a company that handles a large quantity of sensitive confidential data, as Defendants do, will develop a Business Continuity Plan (BCP) that involves three crucial steps. First, the company must identify all threats to its information security, including internal vulnerabilities. This means determining how threats such as cyberattacks or could impact the entity’s business and the individuals whose sensitive information it maintains. Second, the entity must take

⁹ <https://www.changehealthcare.com/>

¹⁰ *Id.*

steps to safeguard its computer systems and sensitive data. This includes enacting security protocols and systems designed to recognize and prevent cyberattacks, as well as reviewing and updating the systems and protocols on a regular basis to ensure they are consistent with the current state of the art and are sufficient to handle the entity's evolving security needs. And third, the entity must ensure that it has the means to repair and restore its systems in the wake of an inevitable cyberattack in order to minimize the disruption to its business, sometimes referred to as a Disaster Recovery Program (DRP). In the healthcare industry this last component is particularly important because the health and well-being of the people who rely on the entity's services may be negatively affected by a cyberattack. Proper preparations include backing up all data to secure, redundant, offsite systems so the information will not be lost, and the business applications can be brought back up to speed and re-populated as quickly as possible. The industry standard for returning business functions to normal is 72 hours. A well designed DRP minimizes the disruption and harm to the company itself, the client companies on whose behalf the company processes the information, and, perhaps more importantly, the individuals whose confidential PHI and PII is affected by the cyberattack.¹¹

24. Here, Defendants failed to create and adhere to a BCP. First, Defendants appear to have been caught completely off guard despite the highly predictable nature of the February 21, 2024, cyberattack, indicating that they had not made a realistic

¹¹ See e.g., ISO/IEC Standard 27001, a standard for information security published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission. <https://www.iso.org/standard/27001>.

assessment of the potential threats to the sensitive confidential data they had been entrusted with.

25. Second, Defendants failed to put adequate security measures in place. Defendants have admitted that BlackCat was able to gain access to Defendants' data systems simply by signing in using stolen credentials. No multifactor authentication was required, so BlackCat easily gained entry. Defendants' security measures are so inadequate that BlackCat was able to gain access to the PHI, PII and other data contained in Defendants' computer systems *undetected for more than a week* before the reported cyberattack on February 21, 2024.¹² Defendants didn't even know BlackCat was prowling around inside their data systems until BlackCat told them so and demanded a ransom. That does not inspire confidence in Defendants' security measures.

26. Multifactor identification is a basic and ubiquitous but highly effective security measure. It works by requiring the user to provide input from at least two of three distinct categories:

- The user's unique knowledge: e.g., a password, PIN, birthdate, or other biographical fact;
- The user's possessions: e.g., a bank card or credit card, USB stick, or smartphone or computer that can receive a unique passcode; and/or
- The user's body: a scan of the user's fingerprint, eye, or face.

27. As everyone who has accessed their bank account or credit card accounts

¹² See <https://www.msn.com/en-us/money/companies/change-healthcare-hackers-broke-in-nine-days-before-ransomware-attack/ar-AA1nsVXI>

online in the last few years knows, most banks or credit card companies require multifactor authentication before a customer can access their account. Yet Defendants failed to take even that basic step to secure the sensitive confidential PII and PHI of millions of United States citizens whose data was affected by the cyberattack. This is a significant breach of the commonly accepted and widely practiced fundamental standard of care for data security in the industry.

Defendants Were Slow to Provide Public Information about the Nature of the Cyberattack.

28. On or around February 21, 2024, UnitedHealth discovered a security breach of Change Healthcare's information technology network (hereinafter, the "Data Breach"). In response to the Data Breach, the company immediately took the impacted systems offline. The shutdown has disrupted the operations of thousands of hospitals, healthcare providers, and pharmacies across the United States.

29. Defendants were slow to come clean about the nature of the cyberattack, describing it as "connectivity issues" in its first dozen public statements about the issue, before finally referencing a "cyber security issue" and admitting they that the so-called connectivity issues were in fact the result of Defendants shutting down their entire system as soon as they became aware of the cyberattack.¹³

30. Adding to the confusion, Defendants failed to notify the patients whose PHI and PII had been affected or whose ability to obtain their medications would be affected. Patients had no idea they might not be able to obtain their medications until they went to

¹³ <https://solution-status.optum.com/incidents/hqpjz25fn3n7>

the pharmacy and were told the transaction could not be processed.

The Change Healthcare Data Breach Cripples the Healthcare Industry.

31. The Data Breach at Change Healthcare has had reverberations across the U.S. healthcare industry, some of which continue to this day. The most negatively impacted are patients who have had trouble accessing their prescriptions and healthcare and now face an increased risk of identity theft.

32. For weeks after the Data Breach, hospitals, healthcare providers, and pharmacies across the U.S. reported that they are unable to process and fill prescriptions through the patients' insurance. This means that the patients didn't receive the medications unless they could afford to pay out of pocket. And healthcare providers were not being paid for the healthcare they were providing. Although Defendants have provided some loans for healthcare providers, the impact on the caregivers, particularly smaller clinics and sole practitioners that cannot sustain their businesses without a steady income stream, has been immense.

The Data Breach has Placed the Confidential Health and Personally Identifiable Information of Millions of Patients at Risk.

33. UnitedHealthcare Group initially claimed that a nation-state actor was responsible for the Data Breach. BlackCat, however, claimed responsibility and stated on its dark web site that it had stolen the confidential PHI and PII of millions of Americans.

34. Specifically, BlackCat said it gained access to 6TB of data, including medical records, and payment and claims information containing PII like names, contact information such as phone numbers and email addresses, and Social Security Numbers.

BlackCat also claimed to have Change Healthcare’s source code and confidential and sensitive information of CVS Caremark, Metlife, Health Net, Federal Medicare, and Tricare.

35. UnitedHealth CEO Andrew Witty admitted in testimony before Congress that UnitedHealth paid a ransom of \$22 million in exchange for an assurance that the data would be returned.¹⁴ Soon thereafter, however, a second dark web entity called RansomHub posted that it had actually executed the cyberattack along with BlackCat, and that BlackCat had pulled an “exit scam,” closing down its dark web site and absconding with the \$22 million ransom payment. RansomHub claims that it, not BlackCat, possesses the PHI and PII exfiltrated from Defendants’ data systems. And now RansomHub has apparently demanded its own ransom payment for the data. News reports indicate that RansomHub has posted samples of the data to prove that it possesses the data and is threatening to sell it to the highest bidder.¹⁵

36. Meanwhile, several terabytes of the sensitive PII and PHI of roughly 100 million United States citizens remains in the control of a shadowy group on the dark web and is still very much at risk as a result of Defendants’ negligence.

37. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 17 C.F.R. § 248.201 (2013). The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific

¹⁴ Witty Testimony at 3

¹⁵ See <https://www.wired.com/story/change-healthcare-ransomhub-data-sale/>.

person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” Id.

38. The United States Government Accountability Office noted in a June 2007 report on data breaches (“GAO Report”) that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in a person’s name.¹⁶ As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim’s credit rating adversely.

39. Accordingly, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.¹⁷

40. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years. According to the GAO Report:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule

¹⁶ See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown (June 2007), United States Government Accountability Office, available at <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

¹⁷ Guide for Assisting Identity Theft Victims, Federal Trade Commission, 4 (September 2013), available at <http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf> (last accessed January 15, 2020).

out all future harm.¹⁸

41. A study by Experian found that the “average total cost” of medical identity theft is “about \$20,000” per incident, and that a majority of victims of medical identity theft are forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.

42. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

43. For all of the above reasons, Plaintiff and the Class members have suffered harm and there is a substantial risk of injury to them that is imminent and concrete and that will continue for years to come.

The Data Breach was a Foreseeable Risk of Which Defendants were on Notice and Could Have Prevented.

44. The healthcare industry is the most frequently targeted industry by cybercriminals. Cyberattacks have doubled from 2016 to 2021, resulting in the exposure of the PHI and PII of millions of Americans.¹⁹

45. Identity thieves and cybercriminals have targeted the medical industry in the last several years because they contain a treasure trove of ultra-sensitive personal data stored on their systems. The medical industry is rife with examples of cybercriminals targeting healthcare providers.

¹⁸ GAO Report at 29.

¹⁹ See <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9856685/#:~:text=In%20this%20cohort%20stud%20y%20of,of%20nearly%2042%20million%20patients> (last visited March 4, 2024).

46. Cyberattacks at medical facilities wreak havoc on patients' lives because they disrupt the medical treatments needed, resulting in delays or cancellations in receiving medical care. Such attacks cause loss of access to patient medical records, including charts, x-rays, and other information needed to treat patients.

47. The Department of Health and Human Services in 2017 released a ransomware fact sheet advising entities covered by HIPPA that “[w]hen electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a ‘disclosure’ not permitted under the HIPAA Privacy Rule.”²⁰

48. Under the HIPAA Privacy Rules, a breach is defined as, “. . . the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.”²¹ Accordingly, attacks like the one at issue are considered a breach under the HIPPA Rules because there was an access of PHI not permitted under the HIPPA Privacy Rule.

49. A ransomware attack is also considered a “Security Incident” under HIPPA. Under the HIPPA Rules, a “Security Incident” is defined as “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.”²²

²⁰ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html>.

²¹ 45 C.F.R. § 164.402.

²² 45 C.F.R. § 164.304.

According to the Department of Health and Human Services, “[t]he presence of ransomware (or any malware) on a covered entity’s or business associate’s computer systems is a security incident under the HIPAA Security Rule.”

50. As early as 2014, the FBI alerted healthcare stakeholders that they were the target of hackers, stating “[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII).”

51. Given the vast amount of PII and PHI Defendants maintain within their data systems and the warnings they received from federal authorities and others, Defendants knew or should have known that they were a target of security threats. They knew that their data was a high-value target for cyberthieves, and that cyberthieves were actively attacking healthcare data systems such as theirs. Defendants’ negligent failure to institute fundamental security measures to protect the PHI and PII of millions of Americans, when a cyberattack was a virtual certainty, left the data completely unguarded and vulnerable to theft.

Defendants, at all Relevant Times, had a Duty to Plaintiff and Class Members to Properly Secure Their PII and PHI

52. Defendants, at all relevant times, had a duty to Plaintiff and Class members to properly secure their PII and PHI, encrypt and maintain such information using industry standard methods, utilize available technology to defend their systems from invasion, act reasonably to prevent foreseeable harms to Plaintiff and Class members, and promptly notify patients when Defendants became aware that patients’ PII and PHI was

compromised.

53. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between them, on the one hand, and Plaintiff and the other Class members, on the other hand. The special relationship arose because Plaintiff and the members of the Class entrusted Defendants (or their providers who entrusted Defendants) with their PII and PHI as part of receiving or paying for medical services and prescription drugs. Defendants had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite their obligations to protect such information. Accordingly, Defendants breached their common law, statutory and other duties owed to Plaintiff and Class members.

54. Defendants' duty to use reasonable security measures also arose under HIPAA. Under HIPAA, Defendants were required to "reasonably protect" PHI from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Plaintiff's and Class members' sensitive information that was compromised in the Data Breach includes PHI, such as provider names, dates of service, medical billing information and potentially other "protected health information" within the meaning of HIPAA.

55. Under HIPPA, Defendants were also required to do the following:

- Ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted. 45 C.F.R. § 164.306(a)(1);
- Implement technical policies and procedures for electronic information

systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights. 45 C.F.R. § 164.312(a)(1);

- Implement policies and procedures to prevent detect, contain, and correct security violations. 45 C.F.R. § 164.308(a)(1)(i);
- Implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports. 45 C.F.R. § 164.308(a)(1)(ii)(D);
- Protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI. 45 C.F.R. § 164.306(a)(2);
- Protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information. 45 C.F.R. § 164.306(a)(3);
- Ensure compliance with HIPAA security standard rules by its workforces. 45 C.F.R. § 164.306(a)(4);
- Train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI. 45 C.F.R. § 164.530(b); and
- Render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by “the use of an

algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR 164.304 definition of encryption).

56. Defendants’ duty to use reasonable security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by entities like Defendant.

57. The Data Breach was a direct and proximate result of Defendants’ failure to: (1) properly safeguard and protect Plaintiff’s and Class members’ PII and PHI from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (2) establish and implement appropriate safeguards to ensure the security and confidentiality of Plaintiff’s and Class members’ PII and PHI; and (3) protect against reasonably foreseeable threats to the security or integrity of such information.

Plaintiff’s Experience

58. Plaintiff Amy Coulson has a medical condition that requires her to take several medications. Failure to take the medications can result in debilitating pain and health risks. The medications are very expensive, even after her insurance has been applied. In order to afford the co-pays, she uses a manufacturer’s co-pay card.

59. After Defendants shut down their systems, Plaintiff’s pharmacy was unable to process her insurance payment or her manufacturer’s co-pay card, leaving her unable

to afford her medications. She was forced to go without her medications for several days. As a result, she suffered debilitating pain. She eventually devised a workaround based on her own knowledge as a nurse and paid out of her own pocket for steroids that were not a perfect solution, came with their own health risks, and added to her out-of-pocket expenses, but provided a small measure of relief from her pain.

60. Plaintiff has spent time and effort researching the data breach and reviewing her financial information to determine if there has been unauthorized activity to her accounts and will perform these activities for the foreseeable future. In addition to not being able to timely obtain her necessary medications, Plaintiff has suffered emotional distress due to the Data Breach and concerns that her PII and PHI is in the hands of cybercriminals and can be ransomed again and otherwise used for identity theft.

CLASS ACTION ALLEGATIONS

61. Plaintiff brings this action individually and on behalf of all other persons similarly situated (the “Nationwide Class”) pursuant to the Federal Rule of Civil Procedure 23(b)(2), (b)(3), and (c)(4).

62. The Nationwide Class is initially defined as follows:

All persons residing in the United States and whose PII and PHI was compromised in the Data Breach announced by Defendants on or around February 21, 2024. Excluded from the proposed Class are Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family members.

63. Plaintiff reserves the right to re-define the Class definition after conducting discovery.

64. Numerosity (Fed. R. Civ. P. 23(a)(1)). The Class members are so numerous that joinder of all members is impracticable. Based on information and belief, the Class includes millions of patients who had their PII and PHI compromised. The parties will be able to identify the exact size of the Class through discovery and Defendants' records.

65. Commonality and Predominance (Fed. R. Civ. P. 23(a)(2)). Common questions of law and fact exist for each of the claims and predominate over questions affecting only individual members of the Class. Questions common to the Class include, but not limited to the following:

- (a) Whether Defendants had a legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiff's and Class members' PII and PHI;
- (b) Whether Defendants breached their legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiff's and Class members' PII and PHI;
- (c) Whether Defendants' conduct, practices, actions, and omissions, resulted in or was the proximate cause of the Data Breach, resulting in the loss of PII and PHI of Plaintiff and Class members;
- (d) Whether Defendants had a legal duty to provide timely and accurate notice of the data breach to Plaintiff and Class members;
- (e) Whether Defendants breached their duty to provide timely and accurate

notice of the Data Breach to Plaintiff and Class members;

- (f) Whether and when Defendants knew or should have known that their systems were vulnerable to attack;
- (g) Whether Defendants violated the Unfair Competition Law;
- (h) Whether Defendants violated the Confidentiality of Medical Information Act;
- (i) Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of their PII and PHI; and
- (j) Whether Plaintiff and Class members are entitled to relief, including damages and equitable relief.

66. Typicality (Fed. R. Civ. P. 23(a)(3)). Pursuant to Rule 23(a)(3), Plaintiff's claims are typical of the claims of the Class members. Plaintiff, like all Class members, had her PII and PHI compromised in the Data Breach and is at an increased risk of harm, including identity theft.

67. Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)). Pursuant to Rule 23(a)(4), Plaintiff and her counsel will fairly and adequately protect the interests of the Class. Plaintiff has no interest antagonistic to, or in conflict with, the interests of the Class members. Plaintiff has retained counsel experienced in prosecuting class actions and data breach cases.

68. Superiority (Fed. R. Civ. P. 23(b)(3)). Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not

economically feasible for individual Class members because the amount of monetary relief available to individual plaintiff is insufficient in the absence of the class action procedure. Separate litigation could yield inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

69. Predominance (Fed. R. Civ. P. 23(b)(3)). Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. Defendants' negligent failure to adequately protect the PII and PHI in its possession had the same effect on all class members: it exposed their confidential data to cyberattack. Defendants breached their duty to Plaintiff and Class Members, and Plaintiff and each Class Member suffered damages as a result of that conduct. Any potential differences in the individual damages suffered by each class member can be addressed by the settlement administrator.

70. Injunctive Relief (Fed. R. Civ. P. 23(b)(2)). Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class.

71. Ascertainability: Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendant's books and records.

CAUSES OF ACTION
COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

72. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

73. Defendants had (and continue to have) a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII and PHI. Defendants also had (and continue to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated (such as in the storage and protection of PII and PHI within their possession, custody, and control).

74. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between them and Plaintiff and Class members, which is recognized by laws including but not limited to HIPAA. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiff and the Class members from a data breach.

75. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII and PHI entrusted to them, including Plaintiff's and Class members' PII and PHI. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting

Plaintiff's and Class members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII and PHI.

76. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached their duties to Plaintiff and Class members by, among other things, failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII and PHI within their possession, custody, and control.

77. Defendants, by and through their negligent actions, inactions, omissions, and want of ordinary care, further breached their duties to Plaintiff and Class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their PII and PHI.

78. But for Defendant's negligent breach of the above-described duties owed to Plaintiff and Class members, their PII and PHI would not have been released, disclosed, and/or disseminated without their authorization.

79. Plaintiff's and Class members' PII and PHI was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and/or disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendants' failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit

their processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Class members' PII and PHI.

80. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this ransomware attack constitute negligence.

81. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the ransomware attack, Plaintiff and Class members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Nationwide Class)

82. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

83. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendants had a duty to

implement reasonable safeguards to protect Plaintiff's and Class Members' PHI.

84. Pursuant to HIPAA, Defendants had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule, by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

85. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

86. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendants had a duty to protect the security and confidentiality of Plaintiff's and Class Members' PII and PHI.

87. Defendants breached their duties to Plaintiff and Class Members under HIPAA, the Federal Trade Commission Act, and the Gramm-Leach-Bliley Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

88. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

89. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

90. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of its duties. Defendants knew or

should have known that it was failing to meet its duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII and PHI.

91. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class)

92. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

93. Plaintiff and Class members' PII and PHI has value that was conferred on Defendants. Moreover, Plaintiff and Class members conferred benefits on Defendants in the form of payments for medical and healthcare services, both directly and indirectly. Defendants had knowledge of the benefits conferred by Plaintiff and Class members and appreciated such benefits. Defendants should have used, in part, the monies Plaintiff and

Class members paid to it, directly and indirectly, to pay the costs of reasonable data privacy and security practices and procedures.

94. Additionally, Defendants utilized Plaintiff and Class members' valuable PII and PHI for their own business purposes and because Plaintiff and Class members bestowed actual value on Defendants, Defendants were obligated to devote sufficient resources to implement reasonable data privacy and security practices and procedures.

95. Plaintiff and Class members have suffered actual damages and harm as a result of Defendants' conduct, inactions, and omissions. Defendants should be required to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds received from Plaintiff and Class members, including damages equaling the difference in value between the medical and healthcare services that included the reasonable data privacy and security practices and procedures Plaintiff and Class members paid for and the medical and healthcare services without the reasonable data privacy and security practices they actually received.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the members of the Class defined above, respectfully request that this Court:

- (a) An order certifying this case as a class action under Federal Rule of Civil Procedure 23, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;
- (b) A judgment awarding Plaintiff and Class members appropriate monetary relief, including actual damages, statutory damages, punitive damages,

equitable relief, restitution, and disgorgement;

(c) An order entering injunctive and declaratory relief as appropriate under the applicable law;

(d) An order awarding Plaintiff and the Class pre-judgment and/or post-judgment interest as prescribed by law;

(e) An order awarding reasonable attorneys' fees and costs as permitted by law; and

(f) Any and all other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial.

Dated: July 25, 2024

LOCKRIDGE GRINDAL NAUEN PLLP

By: s/ Karen H. Riebel

Karen H. Riebel (MN #0219770)
Kate M. Baxter-Kauf (MN #0392037)
Emma Ritter Gordon (MN #0404000)
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
khriebel@locklaw.com
kmbaxter-kauf@lockaw.com
erittergordon@locklaw.com

/s/ Joseph R. Saveri
Joseph R. Saveri
Joseph R. Saveri, Cal. Bar No. 130064*
Cadio Zirpoli, Cal. Bar No. 179108*
Kevin E. Rayhill, Cal. Bar No. 267496*
Itak Moradi, Cal. Bar No. 310537*
JOSEPH SAVERI LAW FIRM, LLP
601 California Street, Suite 1505

San Francisco, California 94108
Telephone: (415) 500-6800
Facsimile: (415) 395-9940
jsaveri@saverilawfirm.com
czirpoli@saverilawfirm.com
krayhill@saverilawfirm.com
imoradi@saverilawfirm.com

* *Pro hac vice* forthcoming.

Attorneys for Plaintiff